#3

PCT/JP2004/008942

日本国特許庁 JAPAN PATENT OFFICE

26.07.2004

Rec'd PCT/PTO 04 APR 2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　６月１９日

出願番号
Application Number: 特願２００３－１７５０８５

[ST. 10/C]: [ＪＰ２００３－１７５０８５]

出願人
Applicant(s): 日本電信電話株式会社

２００４年　９月　２日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３０７８６６７

【書類名】　特許願

【整理番号】　NTTH155516

【あて先】　特許庁長官殿

【国際特許分類】　H04L 12/00

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　小野　久美子

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　立元　慎也

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　坂谷　精一

【特許出願人】

【識別番号】　000004226

【氏名又は名称】　日本電信電話株式会社

【代理人】

【識別番号】　100077274

【弁理士】

【氏名又は名称】　磯村　雅俊

【電話番号】　03-3348-5035

【選任した代理人】

【識別番号】　100102587

【弁理士】

【氏名又は名称】　渡邉　昌幸

【電話番号】　03-3348-5035

【手数料の表示】

【予納台帳番号】　013402

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9701395

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　セッション制御サーバ、通信装置、通信システムおよび通信方法、ならびにそのプログラムと記録媒体

【特許請求の範囲】

【請求項１】　ネットワークを介してセッション制御サーバと通信可能に接続され、前記セッション制御サーバとの間で信号送受信により他の通信装置とのセッションを確立する通信装置において、

非対称鍵ペアを作成する手段と、

前記セッション制御サーバに対して前記非対称鍵ペアのうちの公開鍵に対する証明書発行を要求する要求手段と、

該セッション制御サーバから公開鍵証明書発行完了の通知を受信する受信手段と、

受信した公開鍵証明書を保管する保管手段と、

該セッション制御サーバに対して該通信装置の位置の登録要求を送信する送信手段と、

該セッション制御サーバから有効期間を含む位置登録完了の通知を受信する受信手段とを備え、

前記位置登録要求と証明書発行要求の一括した要求を送信することを特徴とする通信装置。

【請求項２】　請求項１記載の通信装置において、

前記公開鍵証明書を保管する保管手段は、位置登録完了通知に含まれる有効期間を、発行された証明書の有効期間として保管することを特徴とする通信装置。

【請求項３】　ネットワークを介してセッション制御サーバと通信可能に接続され、前記セッション制御サーバとの間で信号送受信により他の通信装置とのセッションを確立する通信装置において、

非対称鍵ペアを保管する手段と、

前記非対称鍵ペアのうちの公開鍵の証明書を保管する保管手段と、

前記セッション制御サーバに対して該公開鍵証明書の登録要求を送信する送信

手段と、

該セッション制御サーバに対して該通信装置の位置の登録要求を送信する送信手段と、

該セッション制御サーバから有効期間を含む位置登録完了の通知を受信する受信手段と

を備えたことを特徴とする通信装置。

【請求項４】　請求項３記載の通信装置において、

前記公開鍵証明書を保管する保管手段は、位置登録完了通知に含まれる有効期間を、発行された証明書の有効期間として保管することを特徴とする通信装置。

【請求項５】　ネットワークを介して複数の通信装置と通信可能に接続され、発信側の通信装置から送信された信号を受信し、受信された信号を着信側の通信装置に送信することで、前記発信側の通信装置と前記着信側の通信装置とのセッションを確立させるセッション制御サーバであって、

前記通信装置からの位置登録要求と、公開鍵に対する証明書発行要求あるいは証明書登録要求の一括した要求を受信する受信手段と、

前記要求を受け付け、公開鍵証明書の発行を行う、あるいは該公開鍵証明書の有効性を確認する手段と、

発行あるいは登録した該公開鍵証明書と位置情報を、有効期間とともに保管する手段と

を備えたことを特徴とするセッション制御サーバ。

【請求項６】　請求項５記載のセッション制御サーバにおいて、

前記公開鍵証明書の問い合せ要求を受信する受信手段と、

該公開鍵証明書の有効性を確認した上で、当該公開鍵証明書を通知する送信手段と

を備えたことを特徴とするセッション制御サーバ。

【請求項７】　ネットワークを介して通信可能に接続され、通信装置相互間でセッションを確立するための通信システムにおいて、

非対称鍵ペアを作成する手段、公開鍵に対する証明書発行の要求を行う要求手段、証明書発行通知を受信する受信手段、公開鍵証明書を保管する保管手段、位

置登録要求を送信する送信手段、および、有効期間を含む位置登録完了通知を受信する手段を備えた通信装置と、

前記通信装置からの位置登録要求を受信する受信手段、公開鍵に対する証明書発行あるいは証明書登録の要求を一括して受け付ける受信手段、証明書を発行あるいは有効性を確認する手段、および、発行あるいは登録した証明書と位置情報を、有効時間とともに保管する保管手段を備えたセッション制御サーバと

を有することを特徴とする通信システム。

【請求項８】　請求項７記載の通信システムにおいて、

前記通信装置は、位置登録完了通知に含まれる有効期間を発行された公開鍵証明書の有効期間として保管する保管手段を備え、

前記セッション制御サーバは、証明書問い合せ要求を受信する受信手段と、証明書通知の送信手段を備えたことを特徴とする通信システム。

【請求項９】　請求項７記載の通信システムにおいて、

前記通信装置は、非対称鍵ペアを保管する手段と、公開鍵証明書の登録要求を送信する送信手段を備え、

前記セッション制御サーバは、証明書問い合せ要求を受信する受信手段と、証明書通知の送信手段を備えたことを特徴とする通信システム。

【請求項１０】　ネットワークを介して通信可能に接続され、通信装置相互間でセッションを確立するための通信方法において、

セッション制御サーバは、通信装置から位置登録と証明書発行の要求信号を受信すると、信号種別を判定し、位置登録要求であれば、証明書発行要求を含むか否かを判定し、発行要求を含む場合には、証明書を発行して、該位置情報と該証明書を管理するとともに、前記通信装置に対して位置情報と証明書発行完了通知の信号を送信することを特徴とする通信方法。

【請求項１１】　ネットワークを介して通信可能に接続され、通信装置相互間でセッションを確立するための通信方法において、

セッション制御サーバは、通信装置から証明書問合せ要求信号を受信すると、セッション制御を行うとともに、自ドメイン宛てか否かを判定し、そうであれば、信号種別を判定し、証明書問合せ要求であれば、証明書があるか否かを判定し

、あれば、該当する証明書を検索し、検索された証明書の有効性を確認して前記通信装置に対して証明書通知を送信し、自ドメイン宛てでない場合には、宛先のセッション制御サーバに該証明書問合せ要求信号を転送することを特徴とする通信方法。

【請求項１２】　ネットワークを介して通信可能に接続され、通信装置相互間でセッションを確立するための通信用プログラムであって、

セッション制御サーバのコンピュータに、通信装置から位置登録と証明書発行の要求信号を受信する手順、信号種別を判定する手順、位置登録要求であれば、証明書発行要求を含むか否かを判定する手順、発行要求を含む場合には、証明書を発行する手順、該位置情報と該証明書を管理する手順、前記通信装置に対して位置情報と証明書発行完了通知の信号を送信する手順を、それぞれ実行させるための通信用プログラム。

【請求項１３】　ネットワークを介して通信可能に接続され、通信装置相互間でセッションを確立するための通信用プログラムであって、

セッション制御サーバのコンピュータに、通信装置から証明書問合せ要求信号を受信する手順、セッション制御を行う手順、自ドメイン宛てか否かを判定する手順、そうであれば、信号種別を判定する手順、証明書問合せ要求であれば、証明書があるか否かを判定する手順、あれば、該当する証明書を検索する手順、検索された証明書の有効性を確認する手順、前記通信装置に対して証明書通知を送信する手順、自ドメイン宛てでない場合には、宛先のセッション制御サーバに該証明書問合せ要求信号を転送する手順を、それぞれ実行させるための通信用プログラム。

【請求項１４】　請求項１２または１３に記載の通信用プログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、電子証明書発行およびその管理を行うセッション制御サーバと、その電子証明書を利用して通信を行う通信装置と、通信システムと、その通信方法

、ならびに、その通信方法を実行させるためのプログラムとそれを記録する記録媒体に関する。

【０００２】

【従来の技術】

従来より、電子証明書の発行サーバ、電子証明書の管理サーバや認証局としては、ＬＤＡＰ（Ｌｉｇｈｔｗａｉｇｔ　Ｄｉｒｅｃｔｏｒｙ　Ａｃｃｅｓｓ　Ｐｒｏｔｏｃｏｌ）サーバや、Ｗｅｂ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）サーバが挙げられる。前者は、Ｘ．５００ベースのディレクトリ管理データベースにアクセスするためのプロトコルであって、ディレクトリサーバ上のディレクトリ情報の作成、変更、削除、検索などの操作が可能である。後者は、インターネット上にハイパーテキストを構築し、あらゆる情報をアクセス可能にすることを目的としており、クライアントとサーバとの通信プロトコルにはＨＴＴＰが用いられる。

これらのサーバの利用方法では、電子証明書の利用者が、暗号化通信を行う場合に、必要に応じて通信相手の電子証明書を取得する必要がある。

また取得した電子証明書について、認証局リンクをたどったり、ＣＲＬ（失効リスト）を取得するなどして、有効性を判断する必要もある。

【０００３】

上記に関しては、インターネットの標準化機関であるＩＥＴＦ（Ｉｎｔｅｒｎｅｔ　Ｅｎｇｉｎｅｅｒｉｎｇ　Ｔａｓｋ　Ｆｏｒｃｅ）がとりまとめている規格書の中で、ＲＦＣ（Ｆｒｅｑｕｅｓｔ　ｆｏｒ　Ｃｏｍｍｅｎｔｓ）２５１１（非特許文献１参照）がある。

【０００４】

【非特許文献１】

ＲＦＣ２５１１Ｉｎｔｅｒｎｅｔ　Ｘ．５０９　Ｃｅｒｔｉｆｉｃａｔｅ　Ｒｅｑｕｅｓｔ　Ｍｅｓｓａｇｅ　Ｆｏｒｍａｔ

【０００５】

【発明が解決しようとする課題】

通信相手が複数の電子証明書を所持し、有効期間も様々である場合、電子証明

書の利用者は、セッションを開始する際に、どの電子証明書を利用するのが適当であるかを判断するために、電子証明書の管理サーバから、通信相手に対応する複数の電子証明書を取得して、各々について有効性を判断する必要があった。

また、有効であると判断した証明書を利用して、信号を送信しても、受信元の通信装置において、その証明書を利用可能な状態に設定していない場合には、受信側で復号化できず、セッション開始処理が遅延するという問題点があった。

さらに、通信相手のデジタル署名に含まれる電子証明書を受信した場合に、受信した証明書が有効か否かを判断するため、ＬＤＡＰサーバに接続する処理などを行う場合には、セッションの開始処理が遅延するという問題点もあった。

【０００６】

（目的）

本発明の目的は、上記のような従来の課題を解決し、セッション通信を行う通信装置に対して有効な電子証明書を配布でき、ユーザへのセッション確立時の有効性確認を容易にすることが可能な電子証明書管理機能を具備するセッション制御サーバ、およびそのサーバを用いて通信を行う通信装置と通信システムと通信方法、ならびにそのプログラムとそのプログラムを記録する記録媒体を提供することにある。

【０００７】

【課題を解決するための手段】

本発明は、次のような機能を有する。

（１）あるユーザＡが、自分の通信装置Ａ’の位置登録要求を行うに当って、非対称鍵ペアを作成し、その鍵ペアの中の公開鍵に対する証明書発行要求と、位置登録要求を一括してセッション制御サーバに送信する（請求項１参照）。

（２）セッション制御サーバが、通信装置Ａ’から上記（１）の要求を受信し、ユーザ認証した上で証明書を発行し、位置情報の有効時間とともに保管する（請求項５参照）。

【０００８】

（３）上記（１）の処理を行った通信装置Ａ’は、上記（２）の処理を行ったセッション制御サーバからの位置登録完了通知と、証明書発行完了通知を、有効時

間とともに受信し、これを保管する（請求項２参照）。

（４）あるユーザＡが、自分の通信装置Ａ’の位置登録要求を行うに当って、非対称鍵ペアとその鍵ペアの中の公開鍵に対する証明書を既に所有し、位置登録要求と、証明書登録要求を、一括してセッション制御サーバに送信する（請求項３参照）。

【０００９】

（５）セッション制御サーバが、通信装置Ａ’から上記（２）の要求を受信し、証明書の有効性を判断して、ユーザ認証を行った上で、証明書の登録を有効時間のある位置登録とともに保管する（請求項５参照）。

（６）上記（４）の処理を行った通信装置Ａ’は、上記（５）の処理を行ったセッション制御サーバからの位置登録完了通知と、証明書発行完了通知を有効時間とともに受信し、これを保管する（請求項４参照）。

【００１０】

（７）通信装置Ｂ’がセッション開始に先立ち、通信相手Ａの公開証明書をセッション制御サーバに対して問い合わせる。

（８）セッション制御サーバは、証明書問い合わせ要求を受信し、その問い合わせ対象の通信相手Ａについて、通信装置Ａ’の公開鍵証明書の有効性を確認し、これを通信装置Ｂ’に通知する（請求項６参照）。

【００１１】

本発明においては、位置情報の管理およびセッション制御を行うサーバが、電子証明書（公開鍵証明書）の管理を行うため、通信装置における実有効性を保証した配布が可能になる。

また、電子証明書の配布時には、位置情報の管理およびセッション制御を行うサーバにより有効性が確認されているため、セッション制御信号内で使用する電子証明書の有効性を、認証局などに問い合わせることなく、確認することが可能になる。

【００１２】

【発明の実施の形態】

以下、本発明の実施の形態を、図面を参照して詳細に説明する。

（システム構成）

図１は、本発明の実施形態に係る通信システムの構成図である。

図１に示すように、通信システム１００は、ネットワーク１０を介して通信可能に接続された１台以上のセッション制御サーバ１０１と、複数の通信装置１０２を含むように構成されている。

また、通信装置１０２は、本発明による手順に従って、セッション制御サーバ１０１を介して暗号化通信により通信を行う。なお、通信システム１００においては、セッション制御サーバ１０１が２台用意されているが、２台に限定されるものではない。また、通信装置１０２が２台用意されているが、２台に限定されるものではない。

【００１３】

なお、本発明においては、通信装置１０２は、パソコン、携帯端末あるいはゲートウェイなどの通信機器を含み、ネットワーク１０の構成は、有線、無線を問わない。

以降は、説明の便宜を図るために、通信装置１０２－１を発信側とし、通信装置１０２－２を着信側として説明する。セッション制御サーバ１０１－１を通信装置１０２－１を収容しているものとし、セッション制御サーバ１０１－２を通信装置１０２－２を収容しているものとして説明する。

セッション制御サーバ１０１－１，１０１－２がそれぞれ通信装置１０２－１と通信装置１０２－２から位置登録要求と公開鍵証明書の発行要求あるいは登録要求を受信し、位置登録情報と公開鍵証明書を保管する。

【００１４】

（通信装置）

図２は、本発明の実施形態に係る通信装置のブロック構成図である。

図２に示すように、通信装置１０２は、信号送信手段１１０、セッション制御手段１１１、位置登録要求手段１１２、位置登録通知受信手段１１３、非対称鍵生成（保管）手段１１４、証明書発行（登録）要求手段１１５、位置情報と公開鍵証明書保管手段１１６、信号受信手段１１７および証明書通知受信手段１１８を含むように構成される。

ここで、１１４は、非対称鍵保管手段であるとともに、非対称鍵生成手段でもあり、また、１１５は証明書登録要求手段であるとともに、証明書発行要求手段でもある。従って、以後は、一方を括弧内にして並記する。なお、１１４，１１５は、これら一方だけの機能を備えたものであってもよい。

【００１５】

通信装置１０２－１は、非対称鍵保管（生成）手段１１４で生成（保管）した公開鍵について、証明書登録（発行）要求手段１１５.で要求信号を作成し、位置登録要求手段１１２で生成された位置登録要求信号とを合わせて、セッション制御手段１１１に送る。

セッション制御手段１１１で生成した信号を、信号送信手段１１０よりセッション制御サーバ１０１に送信する。

その後、セッション制御サーバ１０１－１から、位置登録完了通知信号を受信し、セッション制御手段１１１にて信号内容を解析し、位置登録通知受信手段１１３に送る。

公開鍵証明書が添付されていれば、証明書通知受信手段１１８で受信し、位置情報と公開鍵証明書保管手段１１６に、位置情報と公開鍵証明書を合わせて保管する。

これにより、通信装置１０２－１が使用可能な公開鍵証明書が入手できた状態となり、公開鍵を使用した暗号化情報を含む信号受信、および、公開鍵証明書を使用したデジタル署名を添付した信号送信が可能となる。

【００１６】

（第１の実施形態）

第１の実施形態は、通信装置１０２－１がセッション制御サーバ１０１－１に対して位置登録＋証明書発行を要求し、セッション制御サーバ１０１－１から位置登録と証明書発行の完了通知を受けるまでのやりとりである。

図４は、図２の通信装置における送信信号例を示す図、および、図５は、図２の通信装置における受信信号例を示す図である。

ここでの通信装置１０２－１の相手方は、勿論、セッション制御サーバ１０１－１である。例えば、図４に示す通信装置１０２－１からの送信信号は、ＲＦＣ

３２６１に準拠したＳＩＰメッセージの１つであるＲＥＧＩＳＴＥＲメソッド４００であって、そのメッセージに通信装置の位置情報が、要望する有効時間と共に設定されている（４０２）。また、公開鍵証明書要求と、ユーザ認証キーも設定されている（４０２）。これらの情報は、機密性を保つために、コンテンツ暗号化鍵で暗号化され、Ｓ／ＭＩＭＥのＥｎｖｅｌｏｐｅｄ－Ｄａｔａ（４０１）として送信される。

コンテンツ暗号化鍵の暗号化のための、鍵暗号化鍵としては、セッション制御サーバ１０１－１の公開鍵を用いてもよいし、セッション制御サーバ１０１－１と通信装置１０２－１の使用者間の事前共有鍵（パスワードなど）を用いてもよい。

【００１７】

図５に示すように、セッション制御サーバ１０１－１からの受信信号は、ＲＥＧＩＳＴＥＲメソッドに対する正常応答２００　ＯＫ（５００）であって、そのメッセージに登録された位置情報と、セッション制御サーバ１０１－１が認めた有効時間が共に設定されている（５０４）。また、公開鍵証明書も設定されている（５０４）。これらの情報は、機密性を保つために、暗号化鍵で暗号化され、ＥｎｖｅｌｏｐｅｄＤａｔａ内に設定されている（５０２）。

信号の復号化には、まず暗号化されたコンテンツ暗号化鍵（５０５）の復号化を行う。

暗号化鍵の復号化には、通信装置１０２－１の秘密鍵を用いてもよいし、セッション制御サーバ１０１－１と通信装置１０２－１の使用者間の事前共有鍵（パスワードなど）を用いてもよい。

復号化したコンテンツ暗号化鍵で、暗号化した情報（５０４）を復号化する。

受信した位置情報と公開鍵証明書は、有効時間とともに、位置情報と公開鍵証明書保管手段１１６に保管される。

改竄を防ぐために、サーバのデジタル署名（５０３）が添付されていれば、その署名を確認してもよい。

【００１８】

(セッション制御サーバ)

図３は、本発明の実施形態に係るセッション制御サーバのブロック図である。

図３に示すように、セッション制御サーバ１０１は、信号受信手段１２０、セッション制御手段１２１、信号送信手段１２２、証明書発行（登録）要求受信手段１２３、証明書発行（有効性確認）手段１２４、位置登録要求受信手段１２５、位置情報と公開鍵証明書保管手段１２６、公開鍵証明書問合せ要求受信手段１２７、および、公開鍵証明書通知送信手段１２８を具備している。

ここで、１２３は、証明書発行要求受信手段と証明書登録要求手段の両方の機能を備えており、１２４は、証明書発行手段と証明書有効性確認手段の両方の機能を備えている。なお、１２３，１２４は、両方の機能のうちの一方だけを備えていてもよい。

【００１９】

通信装置１０２－１からの位置登録要求信号を、信号受信手段１２０より受信する。受信した位置登録要求信号は、セッション制御手段１２１で位置登録要求信号であると分析されると、位置登録要求受信手段１２５に送られる。

位置登録要求手段１２５にて、ユーザ認証正常終了後、証明書発行要求が添付されていると判断されると、証明書発行要求受信手段１２３に必要な情報を提供する。証明書発行要求受信手段１２３は、要求内容が正当であることを確認し、証明書発行手段１２４にて、ユーザに対する証明書発行を行う。

発行した証明書と位置情報は、位置情報と公開証明書保管手段１２６にて保管される。

セッション制御手段１２１で、位置情報と公開鍵証明書の情報を含めた応答信号を生成し、通信装置１０２－１に信号送信する。

【００２０】

（第２の実施形態）

第２の実施形態は、セッション制御サーバ１０１－１が、通信装置１０２－１から位置登録＋証明書発行の要求を受け、通信装置１０２－１に位置登録と証明書発行の完了通知を送信するまでのやりとりである。

図４および図５は、前述のように、通信装置１０２－１からセッション制御サーバ１０１－１に送信する信号例と通信装置１０２－１がセッション制御サーバ

１０１－１から受信する信号例であったので、セッション制御サーバ１０１－１から通信装置１０２－１に送信する信号例が図５、通信装置１０２－１から受信する信号例が図４になる。

【００２１】

図４に示すように、例えば、セッション制御サーバ１０１－１が通信装置１０２－１から受信した信号が、ＲＦＣ３２６１に準拠したＳＩＰメッセージの１つであるＲＥＧＩＳＴＥＲメソッドであって、そのメッセージに通信装置の位置情報が有効時間と共に設定されている（４０２）。また、公開鍵証明書要求と、ユーザ認証キーも設定されている（４０２）。これらの情報は、機密性を保つために、暗号化鍵で暗号化されている。

【００２２】

コンテンツ暗号化鍵を取得するために、まず、暗号化されたコンテンツ暗号化鍵の復号化を行う。

セッション制御サーバ１０１－１の秘密鍵を用いてもよいし、セッション制御サーバ１０１－１と通信装置１０２－１の使用者間の事前共有鍵（パスワードなど）を用いてもよい。

復号化して取得された暗号化鍵を用いて、暗号化された情報の復号化を行う。

復号化して取得された位置情報登録要求、ユーザ認証キー、証明書発行要求を得る。

ユーザ認証後、証明書発行要求が正当であることを確認し、セッション制御サーバ１０１－１が発行元となる公開鍵証明書を発行する。

発行した公開鍵証明書の有効期限（５０４）は、位置情報の有効期限と同一に設定する。

そして、位置情報と公開鍵証明書を有効期限とともに保管する。

【００２３】

図５に示すように、ＲＥＧＩＳＴＥＲメソッドに対する正常応答２００　ＯＫ（５００）に、登録された位置情報と、セッション制御サーバ１０１－１が認めた有効時間を共に設定する（５０４）。また、公開鍵証明書も設定する（５０４）。これらの情報は、機密性を保つために、暗号化鍵で暗号化する。信号の暗号

化には、暗号化鍵を生成し、その暗号化鍵の暗号化には、通信装置１０２－１の公開鍵を用いてもよいし、セッション制御サーバ１０１－１と通信装置１０２－１の使用者間の事前共有鍵（パスワードなど）を用いてもよい。

このように生成した信号を、通信装置１０２－１に送信する。

【００２４】

図８は、第２の実施形態に係る通信装置の位置登録と証明書発行処理のフローチャートである。

通信装置から送信する信号について、暗号化・復号化などが行われるが、ここではその処理は記載を省略している。

まず、通信装置１０２－１は、通信装置１０２－１の位置登録要求を行うため、非対称鍵ペアを作成し、その鍵ペアの中の公開鍵に対する証明書発行要求と、位置登録要求を一括して、位置登録＋証明書発行要求信号をセッション制御サーバ１０１－１に送信する（５１）（８－①）。セッション制御サーバ１０１－１は、この信号を受信し（５２）、セッション制御を行い（５３）、信号種別を判定して（５４）、位置登録要求であれば、位置登録要求を受信し（５５）、証明書発行要求があるか否かを判定し（５６）、証明書発行要求がなければ、位置情報＋証明書を管理する（５９）。また、証明書発行要求があれば、証明書発行要求を受信し（５７）、証明書を発行し（５８）、位置情報＋証明書を管理する（５９）。そして、セッション制御を行い（６０）、通信装置１０２－１に信号送信する（６１）（８－②）。通信装置１０２－１は、位置登録＋証明書発行完了通知を受信する（６２）。

【００２５】

（第３の実施形態）

第３の実施形態は、他のセッション制御サーバ１０１－２が通信装置１０２－２から受信した信号が、ＳＩＰに準拠したＳＩＰメッセージの１つであるＯＰＴＩＯＮＳメソッドであって、そのメッセージに通信装置１０２－１の公開鍵証明書問合せ要求が設定されている場合のやりとりである。

図６は、図３のセッション制御サーバの受信信号例を示す図であり、図７は、同じくセッション制御サーバの送信信号例を示す図である。

問合せ内容の改竄を防止するために、通信装置１０２－２のデジタル署名、ならびに署名検証のための通信装置１０２－２の公開鍵証明書が設定されている（６０４）。セッション制御サーバ１０１－２は、ＯＰＴＩＯＮＳメソッドのＲｅｑｕｅｓｔ－ＵＲＩに設定されているドメイン名を見て、自ドメイン宛のメソッドか否かを判定する。自ドメインでない場合には、ドメイン名を示すセッション制御サーバ１０１－１に送信する。

【００２６】

セッション制御サーバ１０１－１は、ＯＰＴＩＯＮＳメソッドを受信して、ＯＰＴＩＯＮＳメソッドのＲｅｑｕｅｓｔ－ＵＲＩに設定されているドメイン名を見て、自ドメイン宛のメソッドか否かを判定する。自ドメイン宛のメソッドであれば、証明書登録要求であるか否かを判別する。証明書登録要求であれば、位置情報と公開鍵証明書を保管手段１２６において、通信装置１０２－１のユーザの位置情報と公開鍵証明書と有効時間を検索し、その時点で有効な情報を取得する。それらを取得した情報を、図７に示すＯＰＴＩＯＮＳメソッドに対する応答２００　ＯＫに設定して、通信装置１０２－２に送信する。

この場合、通信装置１０２－２に直接、送信することもできるが、ここではセッション制御サーバ１０１－２を経由して送信する。

【００２７】

図９は、本発明の第３の実施形態に係る証明書問い合せ処理のフローチャートである。

通信装置１０２－２は、証明書問合せ要求信号をセッション制御サーバ１０１－２に送信する（８１）（９－①）。セッション制御サーバ１０１－２は、信号を受信すると（８２）、セッション制御を行い（８３）、自ドメイン宛か否かを判定し（８４）、自ドメイン宛でなければ、セッション制御を行って（８９）、該当するセッション制御サーバに送信する（９０）。この場合、宛先であるセッション制御サーバ１０１－１に転送する（９－②）。自ドメイン宛であれば、信号種別を判定し（８５）、証明書問合せ要求であれば、証明書問合せ要求を受信し（８６）、証明書があるか否かを判定し（８７）、証明書があれば、証明書の通知を行い（８８）、セッション制御を行って（８９）、通信装置１０２－２に

信号送信する（９０）（９－④）。

【００２８】

セッション制御サーバ１０１－１は、その信号を受信し（９１）、セッション制御を行い（９２）、自ドメイン宛であるか否かを判定し（９３）、自ドメイン宛でなければ、セッション制御を行って（９８）、セッション制御サーバ１０１－２に送信するか（９９）、廃棄する。自ドメイン宛であれば、信号種別を判定し（９４）、証明書問合せ要求であれば、証明書問合せ要求を受信する（９５）。証明書があるか否かを判定し（９６）、あれば、証明書通知を行い（９７）、セッション制御を行って（９８）、セッション制御サーバ１０１－２に信号送信する（９９）（９－③）。

セッション制御サーバ１０１－２は、これを受信すると（８２）、セッション制御を行い（８３）、自ドメイン宛でないので、宛先である通信装置１０２に対して信号送信する（９０）（９－④）。通信装置１０２－２は、この証明書通知を受信する（１００）。

【００２９】

このように、本実施形態に係る通信方法では、通信装置で有効な公開鍵証明書をセッション制御サーバで管理することで、セッション通信で利用可能な電子証明書（公開鍵証明書）の配布・流通が可能となる。

また、セッション制御サーバによる電子証明書の配布時に、セッション制御サバにより有効性が確認されているため、セッション制御信号内で使用する電子証明書の有効性を、認証局などに問い合せることなく、確認することが可能となる。

なお、図８および図９の動作フローをプログラム化した後、これらのプログラムをＣＤ－ＲＯＭなどの記録媒体に格納しておけば、プログラムの販売や貸与の場合に便利であり、また、セッション制御サーバとなるコンピュータや、通信装置のコンピュータにこの記録媒体を装着して、プログラムをインストールし、プログラムを実行させることにより、本発明を容易に実現することができる。

【００３０】

【発明の効果】

以上説明したように、本発明によれば、通信装置間の機密性の高い信号送受信のために必要な電子証明書（公開鍵証明書）を、セッション制御サーバが通信装置対応の有効性を確認した上で、これを管理するので、実利用可能な電子証明書の配布が可能であり、ユーザへのセッション確立時の有効性確認が容易となる。

【図面の簡単な説明】

【図１】

本発明の実施形態に係る通信システムの構成図である。

【図２】

図１における通信装置の詳細ブロック構成図である。

【図３】

図１におけるセッション制御サーバの詳細ブロック構成図である。

【図４】

本発明の第１の実施形態に係る通信装置の送信信号例を示す図である。

【図５】

本発明の第１の実施形態に係る通信装置の受信信号例を示す図である。

【図６】

本発明の第３の実施形態に係るセッション制御サーバの受信信号例を示す図である。

【図７】

本発明の第３の実施形態に係るセッション制御サーバの送信信号例を示す図である。

【図８】

本発明の第２の実施形態に係るセッション制御サーバと通信装置の処理フローチャートである。

【図９】

本発明の第３の実施形態に係るセッション制御サーバと通信装置の処理フローチャートである。

【符号の説明】

１０…ネットワーク、１０１…セッション制御サーバ、１０２…通信装置、

１０１－１…通信装置１０２－１を収容するセッション制御サーバ、

１０１－２…通信装置１０２－２を収容するセッション制御サーバ、

１０２－１…発信側通信装置、１０２－２…着信側通信装置、

１１０…信号送信手段、１１１…セッション制御手段、

１１２…位置登録要求手段、１１３…位置登録完了通知受信手段、

１１４…非対称鍵生成（保管）手段、１１５…証明書発行（登録）手段、

１１６…位置情報と公開鍵証明書保管手段、１１７…信号受信手段、

１１８…証明書通知受信手段、１２０…信号受信手段、

１２１…セッション制御手段、１２２…信号送信手段、

１２３…証明書登録要求受信手段、１２４…証明書有効性確認手段、

１２５…位置登録要求受信手段、１２６…位置情報と公開鍵証明書保管手段、

１２７…証明書問合せ要求受信手段、１２８…証明書通知手段、

４００～４０３…証明書発行要求の信号例の各領域、

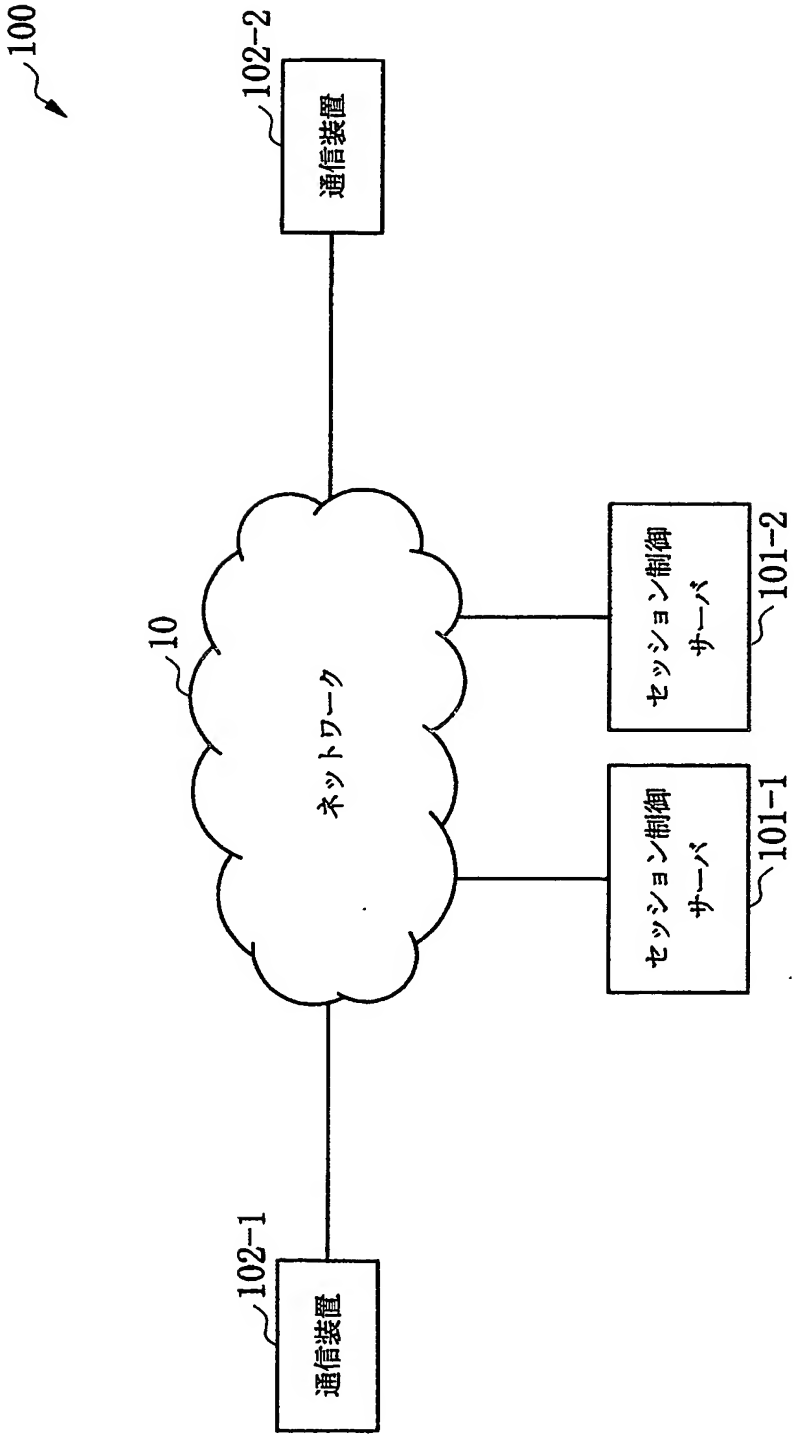
５００～５０５…証明書発行の信号例の各領域、

６００～６０４…証明書問合せ要求の信号例の各領域、

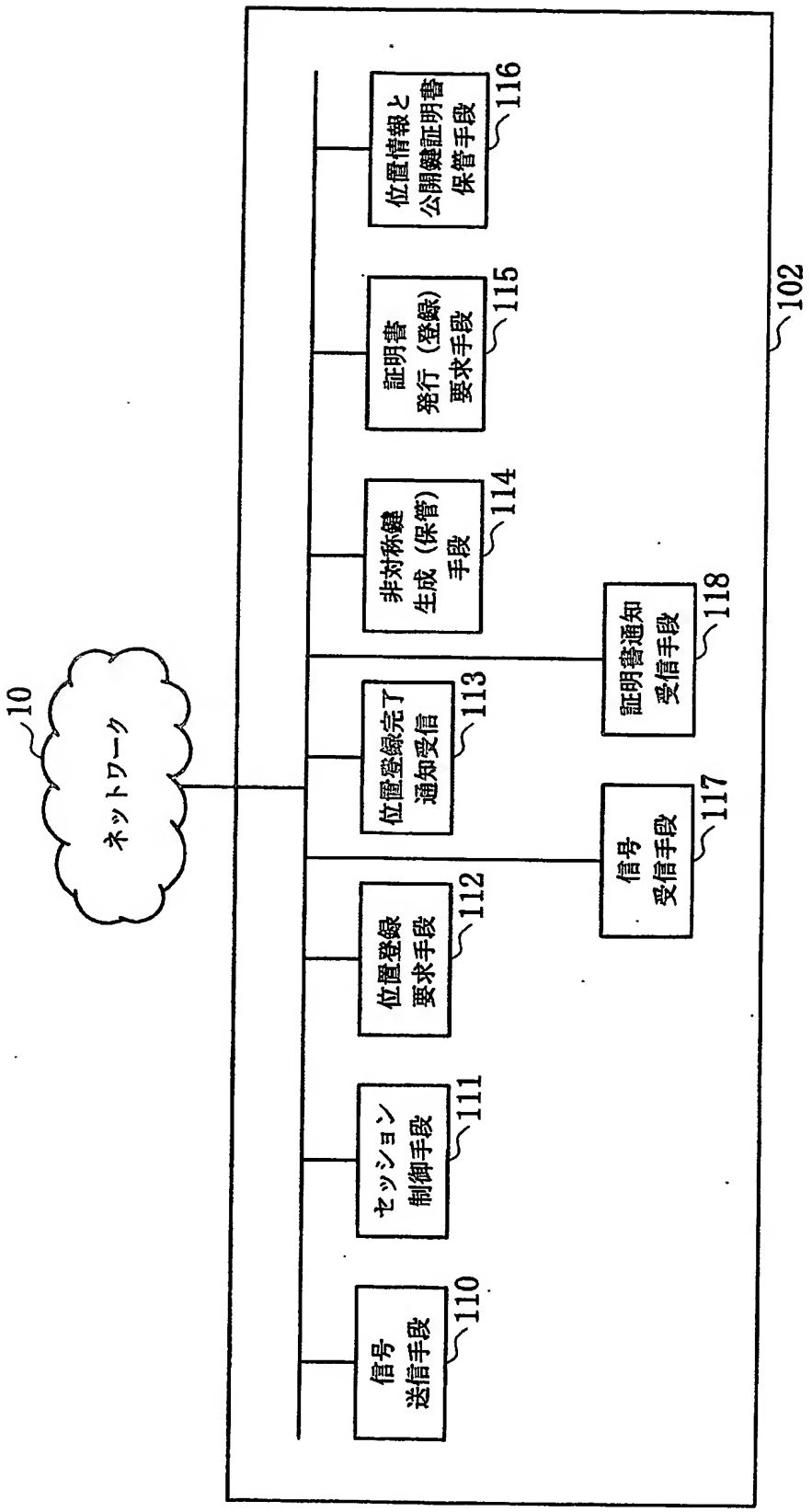
７００～７０５…証明書通知の信号例の各領域。

【書類名】　図面

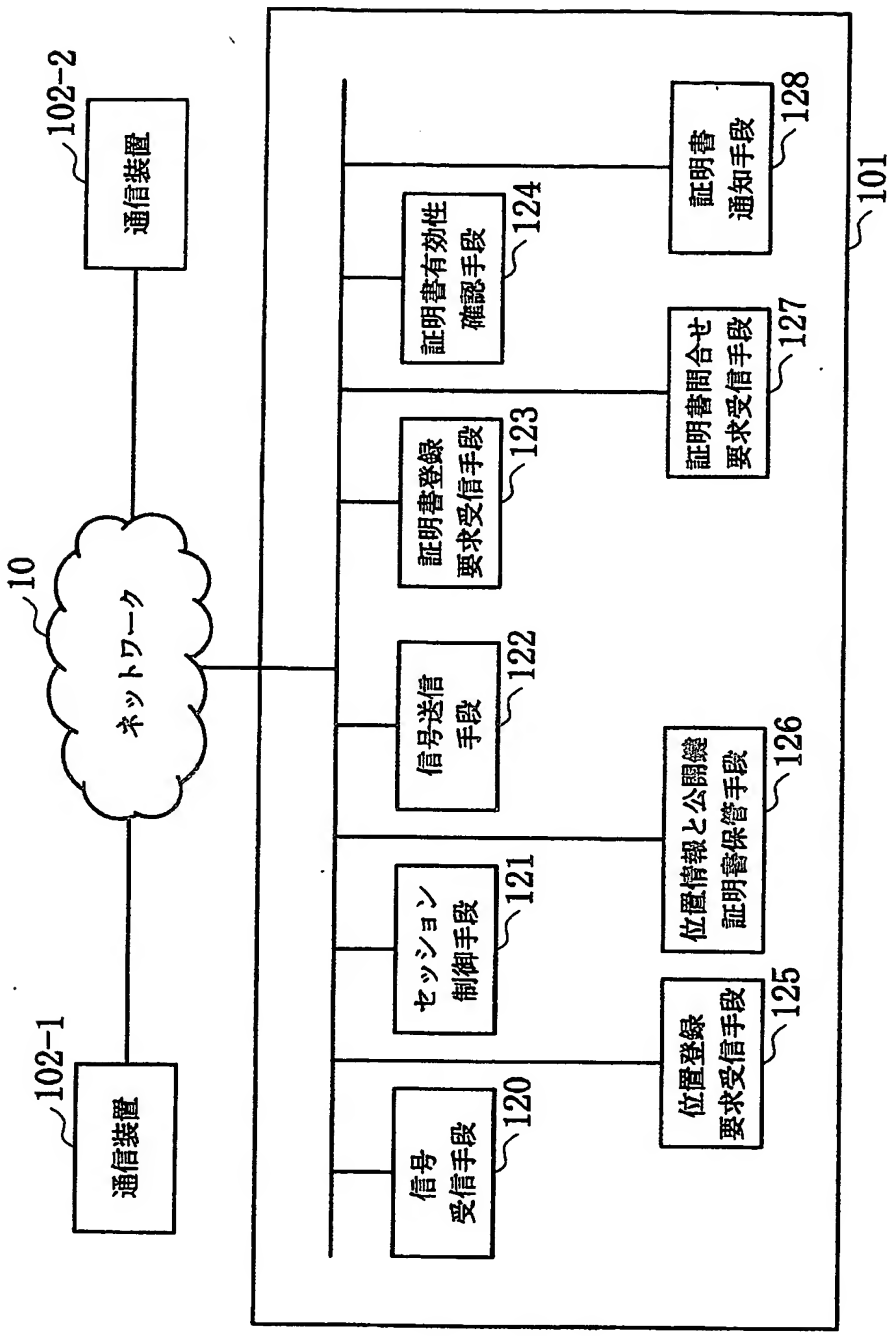
【図１】


100
102-2
通信装置
10
ネットワーク
セッション制御サーバ
101-2
セッション制御サーバ
101-1
102-1
通信装置

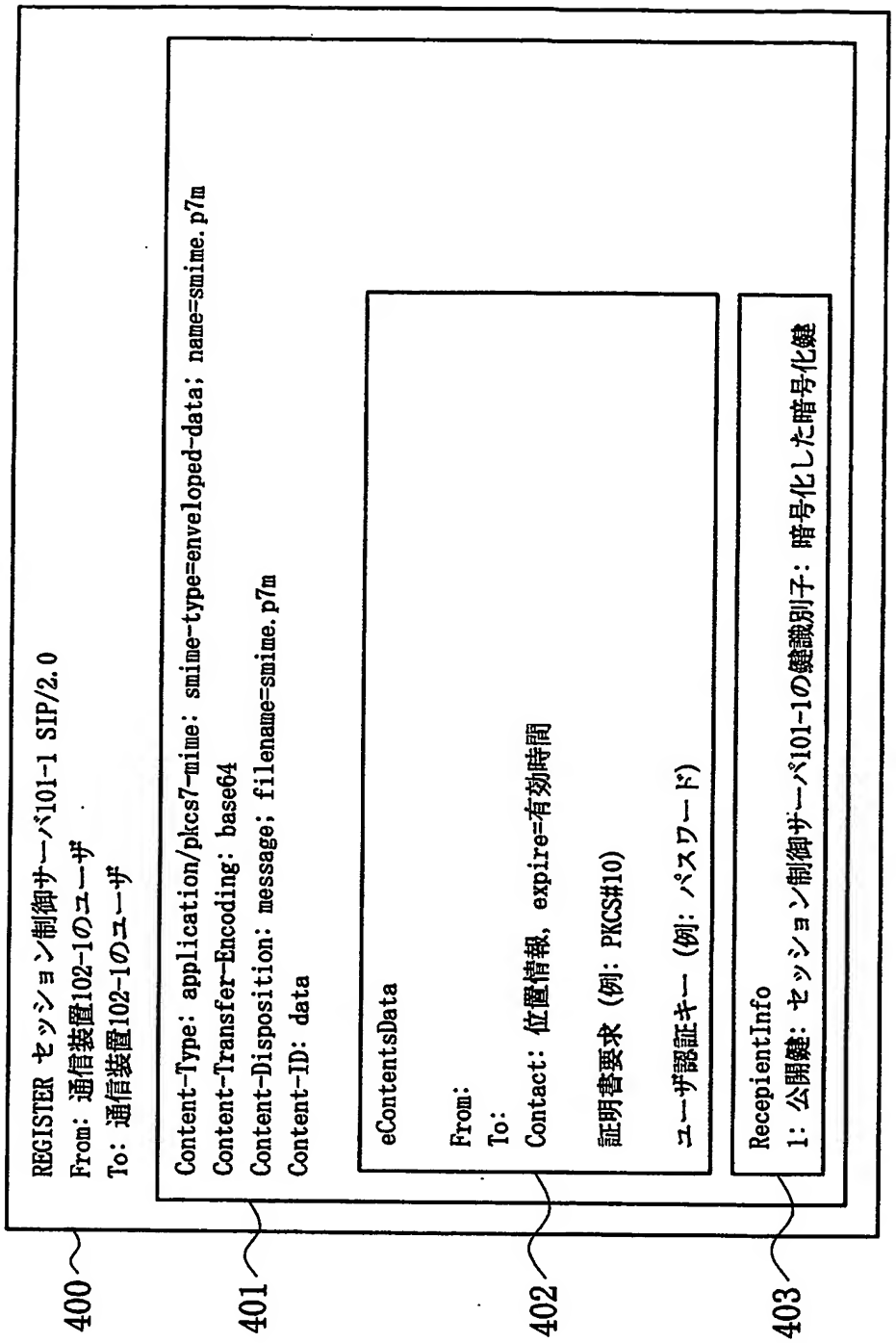
【図２】


10
ネットワーク
102
信号
送信手段
110
セッション
制御手段
111
位置登録
要求手段
112
位置登録完了
通知受信
113
非対称鍵
生成（保管）
手段
114
証明書
発行（登録）
要求手段
115
位置情報と
公開鍵証明書
保管手段
116
信号
受信手段
117
証明書通知
受信手段
118

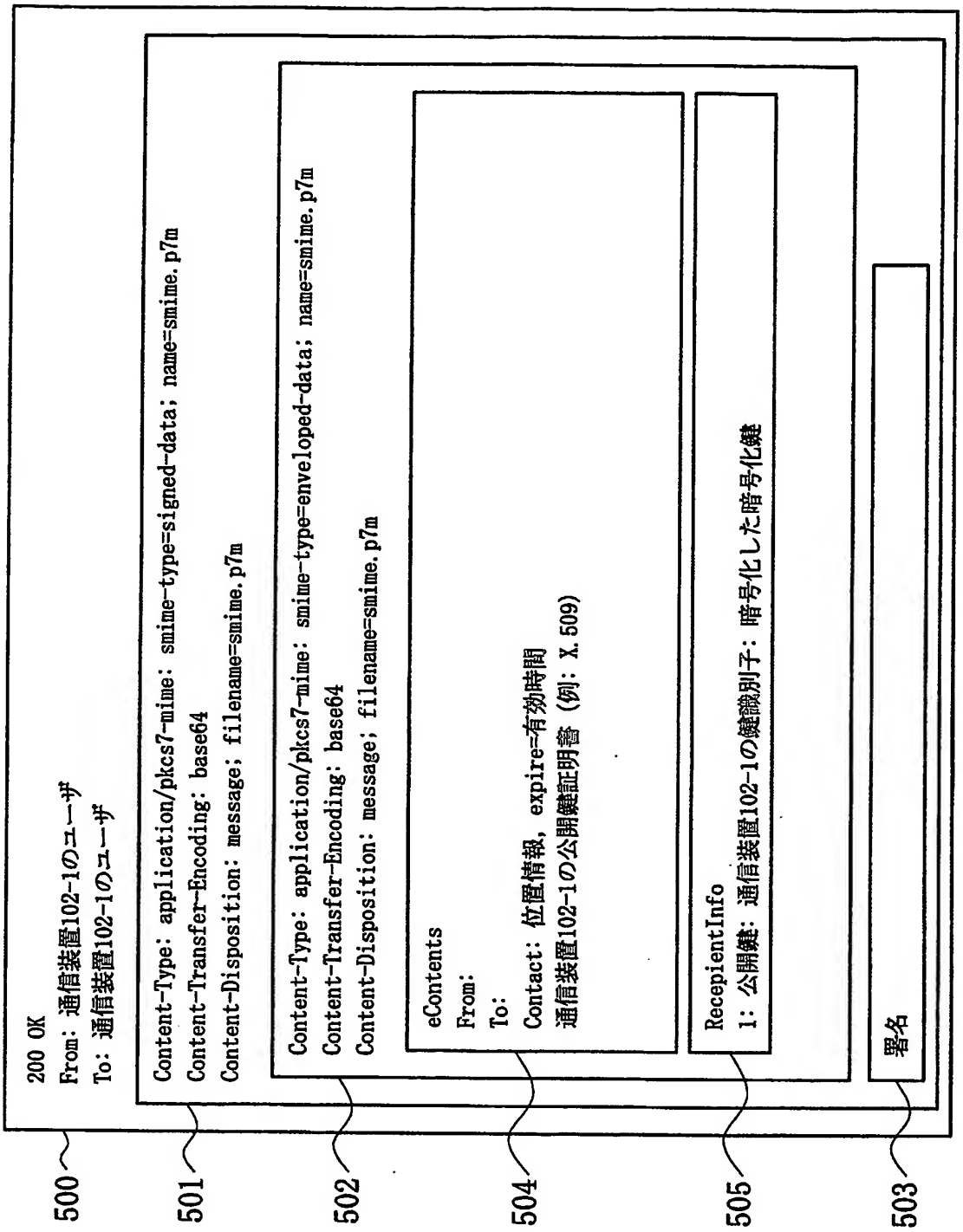
【図３】


102-2
通信装置
102-1
通信装置
10
ネットワーク
101
信号受信手段
120
セッション制御手段
121
信号送信手段
122
証明書登録要求受信手段
123
証明書有効性確認手段
124
位置登録要求受信手段
125
位置情報と公開鍵証明書保管手段
126
証明書問合せ要求受信手段
127
証明書通知手段
128

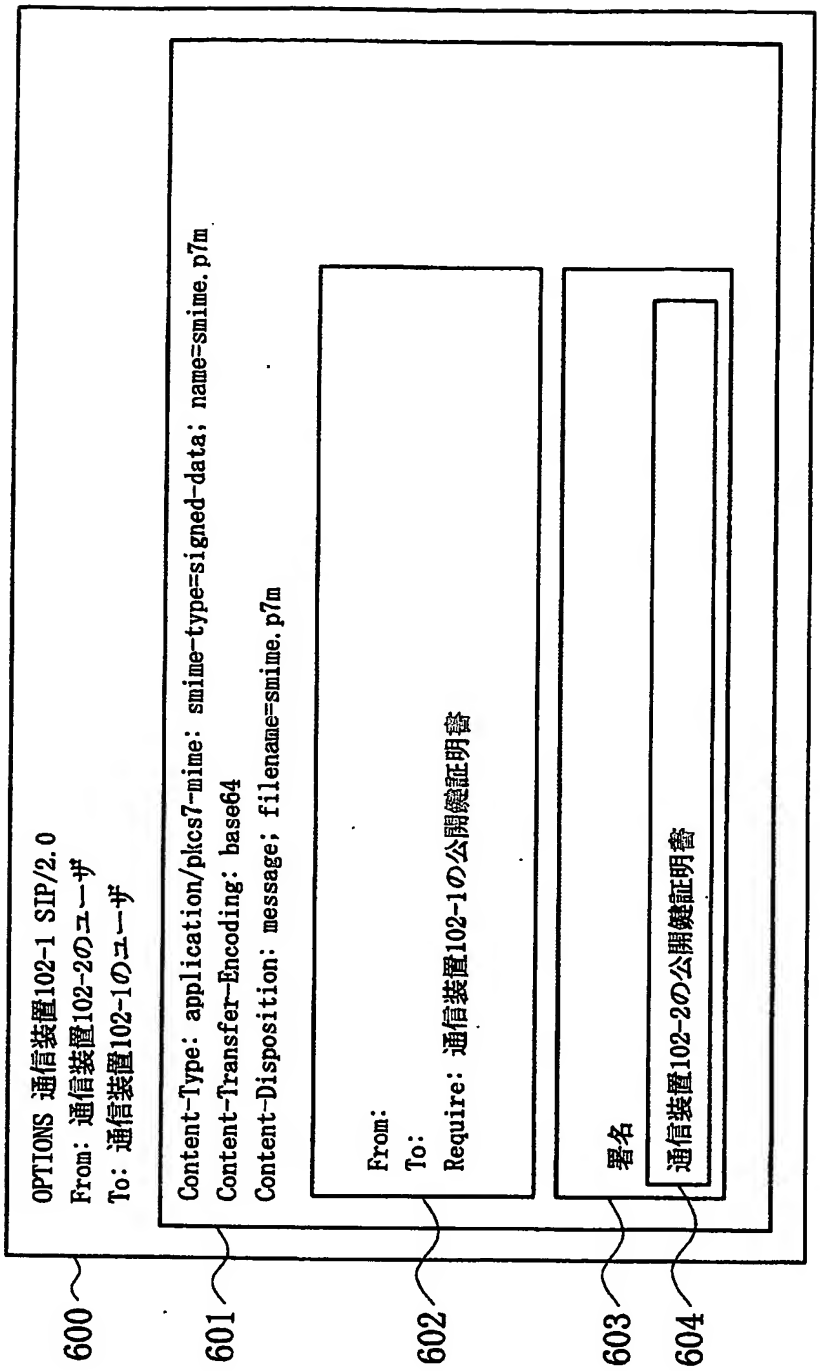
【図４】


REGISTER セッション制御サーバ101-1 SIP/2.0
From: 通信装置102-1のユーザ
To: 通信装置102-1のユーザ
Content-Type: application/pkcs7-mime; smime-type=enveloped-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: message; filename=smime.p7m
Content-ID: data
eContentsData
From:
To:
Contact: 位置情報, expire=有効時間
証明書要求 (例: PKCS#10)
ユーザ認証キー (例: パスワード)
RecepientInfo
1: 公開鍵: セッション制御サーバ101-1の鍵識別子: 暗号化した暗号化鍵
400
401
402
403

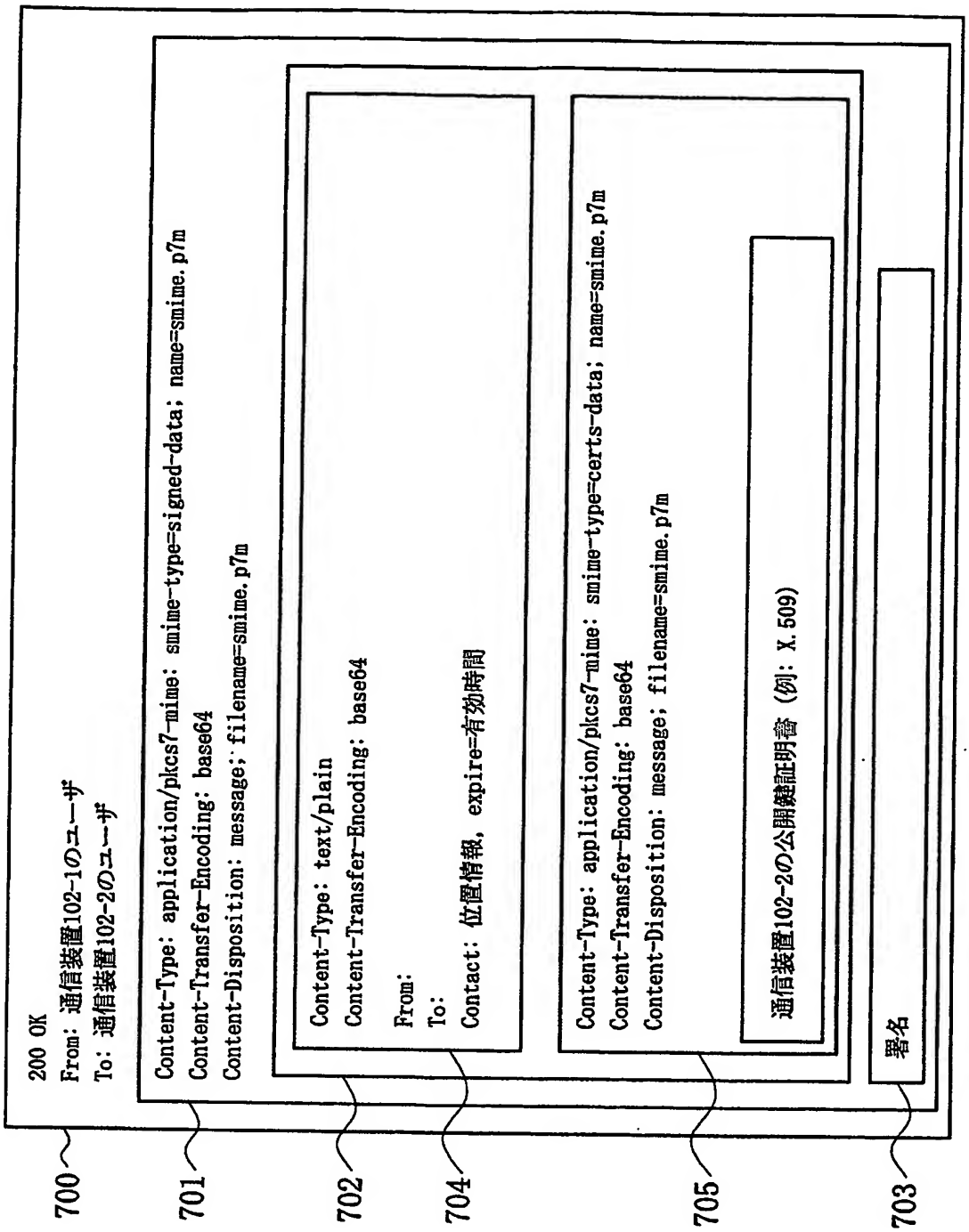
【図５】


200 OK
From: 通信装置102-1のユーザ
To: 通信装置102-1のユーザ
Content-Type: application/pkcs7-mime; smime-type=signed-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: message; filename=smime.p7m
Content-Type: application/pkcs7-mime; smime-type=enveloped-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: message; filename=smime.p7m
eContents
From:
To:
Contact: 位置情報, expire=有効時間
通信装置102-1の公開鍵証明書 (例: X.509)
RecepientInfo
1: 公開鍵: 通信装置102-1の鍵識別子: 暗号化した暗号化鍵
署名
500
501
502
504
505
503

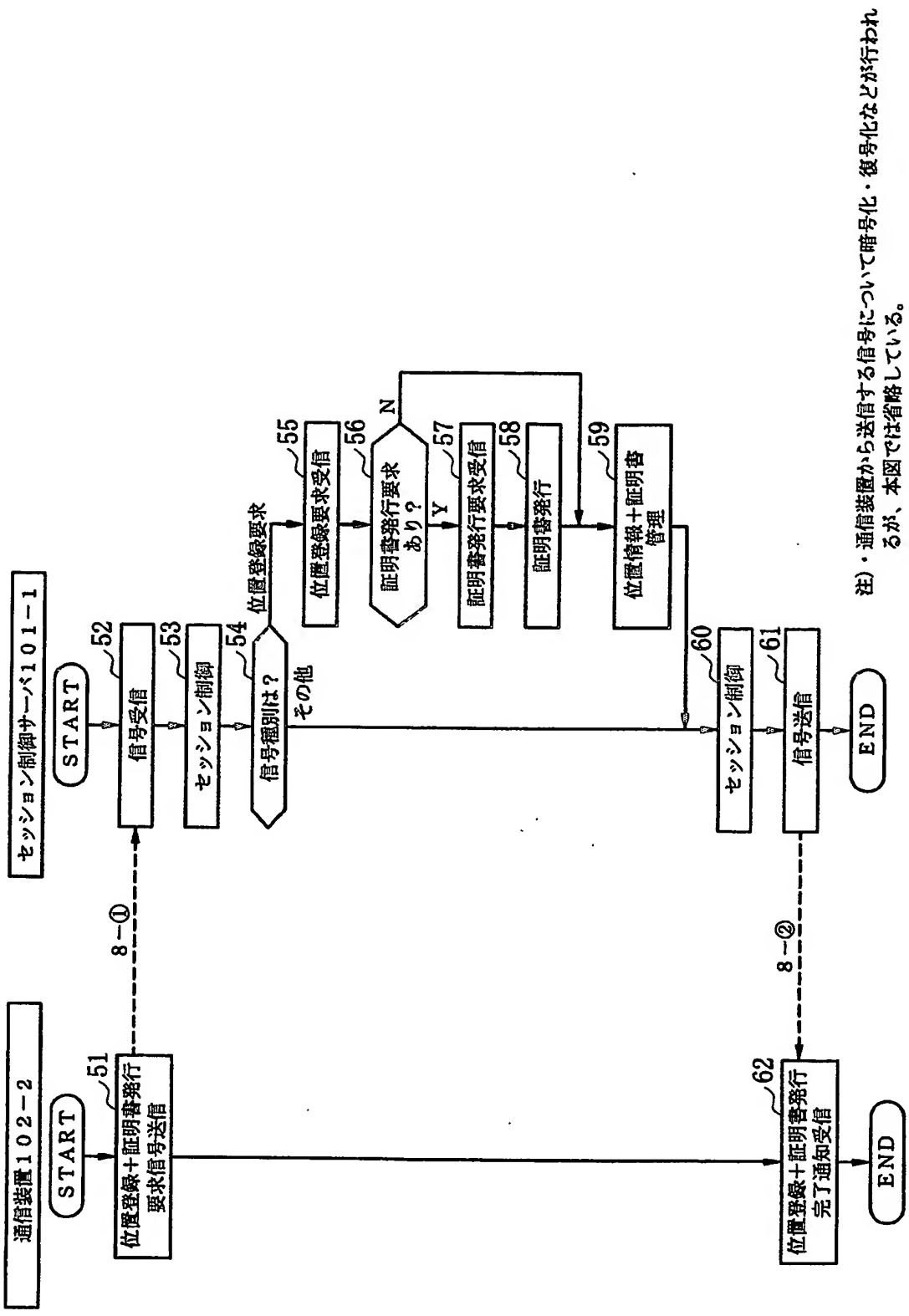
【図６】


OPTIONS 通信装置102-1 SIP/2.0
From: 通信装置102-2のユーザ
To: 通信装置102-1のユーザ
Content-Type: application/pkcs7-mime; smime-type=signed-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: message; filename=smime.p7m
From:
To:
Require: 通信装置102-1の公開鍵証明書
署名
通信装置102-2の公開鍵証明書
600
601
602
603
604

【図７】

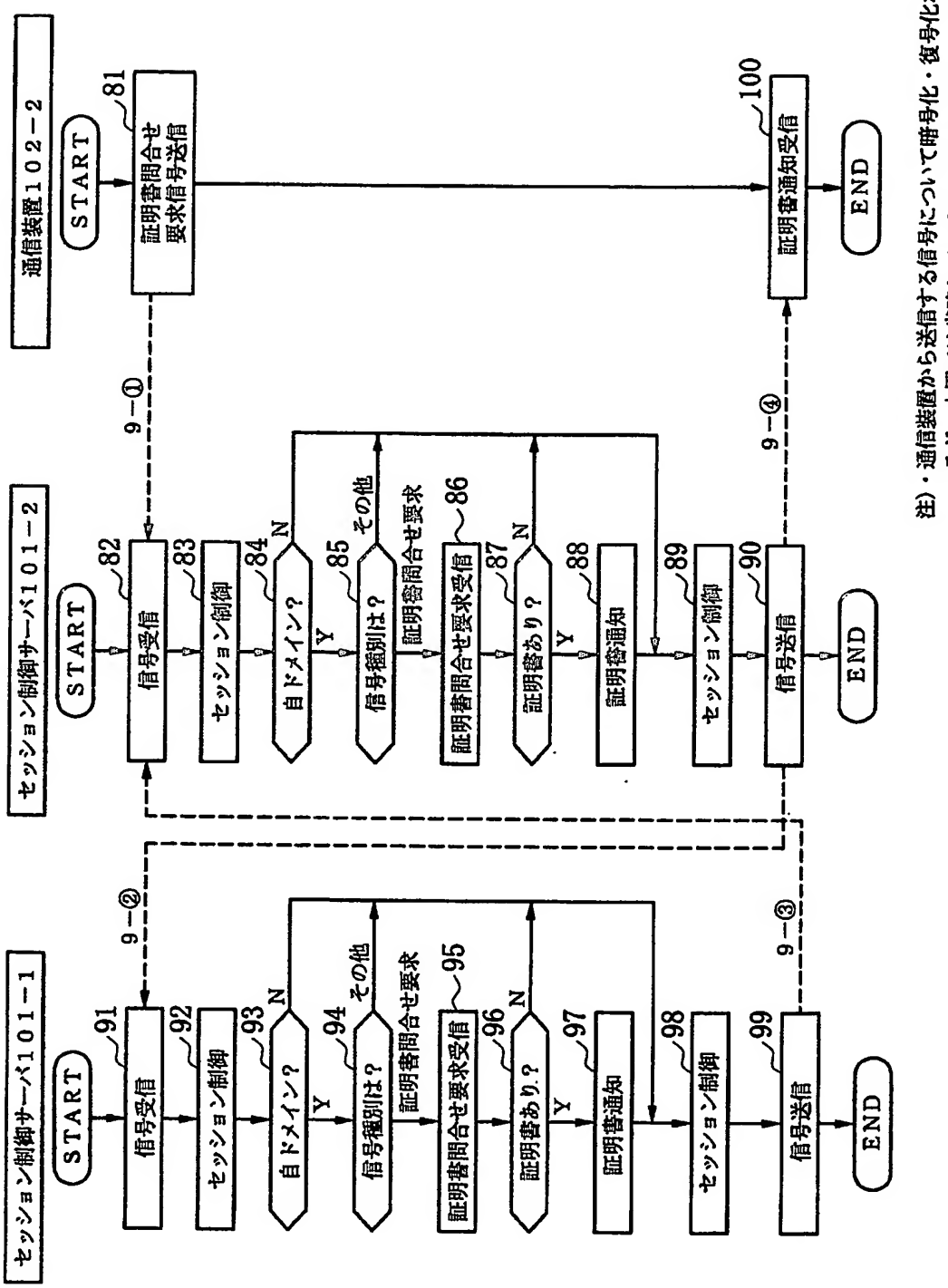

200 OK
From: 通信装置102-1のユーザ
To: 通信装置102-2のユーザ
Content-Type: application/pkcs7-mime; smime-type=signed-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: message; filename=smime.p7m
Content-Type: text/plain
Content-Transfer-Encoding: base64
From:
To:
Contact: 位置情報，expire=有効時間
Content-Type: application/pkcs7-mime; smime-type=certs-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: message; filename=smime.p7m
通信装置102-2の公開鍵証明書（例：X.509）
署名
700
701
702
704
705
703

【図８】



注）・通信装置から送信する信号について暗号化・復号化などが行われるが、本図では省略している。

【図９】



注）・通信装置から送信する信号について暗号化・復号化などが行われるが、本図では省略している。

【書類名】　　要約書

【要約】

【課題】実利用可能な電子証明書の配布が可能であり、ユーザへのセッション確立時の有効性確認を容易にする。

【解決手段】あるユーザが通信装置１０２－１の位置登録要求を行うため、非対称鍵ペアを作成し、その鍵ペアの中の公開鍵に対する証明書発行要求と、位置登録要求を一括してセッション制御サーバ１０１－１に送信する。セッション制御サーバ１０１－１が要求を受信し、ユーザ認証した上で証明書を発行し、位置情報の有効時間とともに保管する。通信装置１０２－１はセッション制御サーバ１０１－１からの位置登録完了通知と、証明書発行完了通知を、有効時間とともに受信し、これを保管する。通信装置１０２－２がセッション開始に先立ち、通信相手１０２－１の公開証明書をセッション制御サーバ１０１－２に対して問い合わせると、これをセッション制御サーバ１０１－１に転送し、セッション制御サーバ１０１－１は、通信相手１０２－１について、公開鍵証明書の有効性を確認し、これを通信装置１０２－２に通知する。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２００３－１７５０８５
受付番号	５０３０１０２６５７２
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１５年　６月２０日

＜認定情報・付加情報＞

【提出日】　平成15年 6月19日

次頁無

出願人履歴情報

識別番号　［０００００４２２６］

１．変更年月日　１９９９年　７月１５日
［変更理由］　住所変更
住　所　東京都千代田区大手町二丁目３番１号
氏　名　日本電信電話株式会社